

**SMARTCARD AUTHENTICATION AND AUTHORIZATION UNIT
ATTACHABLE TO A PDA, COMPUTER, CELL PHONE, OR THE LIKE**

REFERENCE TO RELATED APPLICATION

This application is a continuation-in-part of U.S. Patent Application Serial No. 10/215,888, filed August 9, 2002, the entire content of which is incorporated herein by reference.

5

FIELD OF THE INVENTION

This invention relates generally to authentication and authorization devices and, in particular, to a portable device that can validate smartcards and other monetary instruments and requests with a high degree of transaction security.

BACKGROUND OF THE INVENTION

10

In the modern world of networked transaction processing, authentication is only way to validate requests for financial services and other demands with any degree of security or data integrity. However, even with the current widespread use of encryption, security codes and personal identification numbers (PINs), existing systems are subject to various types of attacks or hacking. Such security breaches may, for example, be carried out through keyboard hooks and other data-sniffing techniques, magnetic card duplicators, smartcard emulators, and so forth.

15

20

At the same, the number of electronic devices applicable to transaction and data processing has grown, including not only dedicated terminals adapted for such uses, but general-purpose computing machinery, personal and digital assistants (PDAs), laptop, palmtop and notebook computers.

Existing authentication devices are deeply connected to computers or other devices such as cable/satellite decoders to validate a particular transaction. As such, these devices represent a single point of attack for hackers who can emulate the authentication device, hook communication between the device and the software stored

inside the "computer." or even record and play communication packets.

To prevent such activities, the industry is working on protocols to enable these devices to operate securely. But protocols have their own weaknesses in the sense that when they are implemented and successfully attacked, patches may become available for
5 widespread use on internet for free.

Accordingly, the need remains for a system which would allow the use of these alternative devices, including portable devices, while, at the same time, affords a level of security which is at least as good, and preferably much higher, than systems currently in use.

10 SUMMARY OF THE INVENTION

The present invention resides in an autonomous and portable smartcard reader device incorporating a high level of embedded security countermeasures. In the preferred embodiment, data transfers are encrypted with two specific input devices, namely a light sensor and PIN or other keyboard entry, and at the output through the use of a dual-tone
15 encoder-decoder. The unit may be used alone or as a plug-in to another device such as a PDA, cell phone, or remote control.

The reader may further be coupled to various biometric or plug-in devices to achieve at least five levels of authentication, namely, (1) the smartcard itself; (2) the smartcard reader; (2) the PIN; (3) private-key cryptography (PKI); and (5) the (optional)
20 biometric device. These five levels account for an extremely strong authentication applicable to public networking on public/private computers, and even on TV (satellite, cable, DVD, CD AUDIO, software applications. Transactions including payments may be carried out without any risk of communication tampering, authentication misconduct or identity theft.

25 In essence, the device is a closed box with only two communication ports. The emulation of the device is therefore extremely complex due to the fact that it involves PKI, hardware serialization for communication and software implementation, in conjunction with a specific hardware embodiment and service usage infrastructure

component that returns a response necessary for each unique transaction.

Another point of convenience involves the existing low-level implementation of the software necessary to work with the authentication process. With existing systems, since each occurrence of authentication requires a low-level implementation of drivers, a potential user cannot connect the device to a public computer such as a web café computer without installing the requisite drivers. According to this invention, the software necessary to validate the transaction need not be a driver or a kernel level application; as such, authentication can come from website with the usage of user level application like and not limited to java, activex, or other languages.

As an alternative to the use of a separate or independent display (CRT or LCD) and keyboard, a plug-in unit may be used. The device is essentially a headset including a smartcard reader, preferably with 2 biometric sensors, one for the voice and the other one for the fingerprint. When the headset is attached, the associated PDA or phone keyboard sends DTMF signals which are recognized by the device. PDA or phone screen can be updated thru a WAP application link to a vocal server.

In the preferred configuration of this embodiment, the biometric headset include a (cryptographic) processor to perform elliptic curves and random number generator. A dedicated ASIC/DSP sends and receives the DTMF/FSK signals. In addition to other advantages, the system can deliver a vocal instruction to the head set. The device is battery operated with a backup. Other features include an atomic time clock and software that can be updated by way of a smartcard javacard or DTMF/FSK. The amount of memory is optional. Policy considerations may also be stored on the smartcard.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGURE 1 is a drawing of a portable smartcard device reader according to the invention;

FIGURE 2 is a drawing which illustrates important aspects of an infrastructure to which the device of Figure 1 is applicable;

FIGURE 3 is a drawing which shows a preferred optical signal according to the

invention associated with the an authentication procedure;

FIGURE 4A is a flow diagram showing the first portion of a preferred device registration process according to the invention;

FIGURE 4B is a flow diagram which illustrates the remaining portion of the preferred device registration process;

FIGURE 5A is the first party of a flow diagram used to illustrate the preferred way in the device is used according to the invention;

FIGURE 5B is a flow diagram illustrating the remaining functional steps of the usage process;

FIGURE 6A is a flow diagram which illustrates a preferred process associated with personal data modification utilizing the device according to the invention;

FIGURE 6B is a flow diagram which continues the personal data modification process according to the invention; and

FIGURE 7 is a drawing of a card reader attachable to a PDA, portable phone or other device, including one or more biometric inputs.

DETAILED DESCRIPTION OF THE INVENTION

Now making reference to the drawings, Figure 1 illustrates the preferred embodiment of the invention in the form of a portable smartcard reader device, indicated generally at 100. The device includes a slot 102 to receive the card 104, and a keyboard 110 enabling passwords, personal identification numbers, and the like to be input by a user. It will be appreciated that although a generic "smartcard" is shown in the figure, in the preferred embodiment, the unit includes its own central-processing unit for transaction management and input/output capability for reading and writing information to various other types of cards including magnetic cards, optical cards, EAROM cards, random-access memory (RAM) cards, and read-on memory (ROM) cards. Nor is the unit limited to the use of a single type of smartcard or other card, since in alternative embodiments, the same unit may recognize multiple card owners and users.

An interface 120 may be provided for connection to a plug-in type of biometric

device such as a fingerprint scanner or other input. Optionally, in the alternative, such plug-in devices may be integrated directly into the apparatus 100. Indeed, although speaker 122 is shown as being remote from the body of the unit, in the preferred embodiment the speaker is integral.

5 Further included in the device 100 is a light sensor 130, described in further detail below, and an output 140 to deliver an encoded signal associated with authentication. As shown in the figure, in the preferred embodiment, the signal is a dual-tone, multi-format (DTMF) signal.

As discussed elsewhere herein, the device incorporates numerous mechanisms to
10 ensure the highest degree of security against hacking and other forms of security attacks. For example, in the preferred embodiment, the device is deactivated in the event that an incorrect PIN number is entered more than a predetermined number of times, which may be adjustable from one instance or more. The system is also preferably capable of sensing and guarding against physical and other forms of corruption, including sensors
15 which detect forces sufficient to break the device or other forms of misconduct.

Other optional capabilities to guard against intrusion include mechanical for preventing the extraction of the card if the PIN/password, fingerprint or other authorization does not correspond to the authorized user. As a further optional, in the event of these other attempts to gain unauthorized access to the unit or components
20 thereof, data stored within the device, whether volatile, or read-only, as well as smartcard or other types of card information may automatically be erased.

In addition to authentication codes and other information associate with a particular instance or transactions, the unit may be equipped with sufficient memory capability to additionally store other types of information, including personal data of the
25 owner of the unit and/or card, including, but not limited to, address, billing address, zip code, social security number, e-mails, web addresses, and so forth.

Given the extent to which certain user information is compiled and stored by the device, an optional feature is the ability to permit new users, as well as the deactivation of other users based upon the receipt of appropriate commands. The activities of particular

users may also be stored and time-stamped, for later readout, either directly through the device or by way of remote access.

The reader may also be automatically updated through the use of codes received on a periodic or occasional example, for example, at the time of each transaction. Such auto-update capabilities may be encrypted with a counter, for example, used to verify reader research, or otherwise used to update algorithms or data stored in memory. As opposed to electrical or wireless remote updates, such information may be received optically or through the use of known or future standard protocols such as bluetooth technology and the like.

Figure 2 is a diagram which illustrates the various environments in which the device 100 operates. Broadly, the system is able to generate a request for an authentication through a wide variety of devices, and receive verification through numerous other diverse types as well. In Figure 2, any device capable of connection to telecommunications infrastructure 210 may receive a request for authentication since, in the preferred embodiment, such requests are generated utilizing the well established dual tone multi-frequency (DTFM) encoder/decoder signal 212. Such devices would include, standard wire telephone 220, cellular telephone 222, any network computer 224 or a numericast network 226 operated to collect and aggregate viewer payments, for example.

In terms of the authentication signal, any television 230 or network computer 232 may participate. Television 230 may, in turn, receive input from any applicable transmission medium, including broadcast 240, satellite 242, and so forth. Equipment originating the information may be derived from a workstation 250 or any other wired or wireless computing device. A network and advertising module 252 may be used to integrated video advertising 254, to add the light signal sensed by sensor 130 of the device 100. The unit 258 may be used to integrate the light signal to broadcast on vertical blanking, MPEG or other protocols to television or monitor 230. Indeed, through the use of a connection between the numericast network device 226 and module 258, a programming signal may be added to the broadcast verification signal, resulting in a comprehensive data feedback loop.

With respect to computer 232, any device capable of connection to the internet 260 or other infrastructure may be used. Devices such as 262 connected to the internet 260 may include the appropriate data enabling the verification signal to be routed from point-to-point, ultimately leading to verification at device 100.

5 The device 100, though shown as an independent unit, may be integrated to any form of existing device, be it a personal digital assistant (PDA), cellular telephone, or even hand-held remote control. In some of these applications, including the remote control, an additional light sensor may not be necessary, since information used to authenticate may already be provided in the form of an existing infrared module
10 associated with any one of a variety of entertainment devices (TV, VCR, tape, DVD, CD audio). In these cases, the additional hardware required by the invention would include the DTMF encoder/decoder, and smartcard reader to permit the acknowledgement of a transaction.

 The data entered into the device 100 may be encrypted or non-encrypted when
15 received. If an encryption mechanism is used, it may be of any type, including public or private key. For example, the name, social security number, or other type of information may be used, depending upon the level of security needed, a technique known as identity-based encryption (IBE).

 As discussed above, the authentication data may be delivered through any type of
20 computer monitor, television, liquid-crystal display (LCD), light-emitting diode or other emitter, operative to generate a high-contrast signal to be received and interpreted by the device 100. Software application would used to generate signals which are transcoded from an analog or other format into a binary, hexadecimal or other digital scheme to enhance reception.

25 In conjunction with the received optical signal, the processor and device 100 preferably further requests additional authentication data through some form of user interface, including the keypad (personal identification number or PIN), biometric authentication, such as a fingerprint, or other applicable security mechanism.

 Once received and stored in internal or external memory, the information is

appropriately decrypted and/or re-encrypted, and sent to any external device (microphone, standard telephone, cellular phone, and so forth) as a dual-tone (DTMF, AFSK, or PL) signal for transactional purposes.

5 The device 100 may operate independently, or as discussed above, may be added a plug-in to an existing device such as a PDA, phone computer, cellular phone, remote control television, keyless entry system, and so forth. Broadly, the interface device coupled to an optoelectronic device incorporating a smartcard reader for the acquisition of optical messages, and a dual-tone multi-decoder (DTMF, AFSK, PL) to send back authentication information, including payment validation, authorization, key opening or
10 other operations.

Now making reference to Figure 3, the preferred embodiment uses a high-contrast black and white image (or any other appropriate color or high-contrast arrangement from an LED, flashing LCD screen, or highly pixelized optical signal). For example, a screen may be used, wherein for example, a black upper signal 302 becomes white, while the
15 black signal 304 becomes black, with the timeframe between the two signals establishing a parity or check sum. In the device 100, an electronic scanning sensor is used including optics which permit the recognition of the black and white images (or other appropriate signal), enabling the smartcard reader data to become available for authentication purposes.

20 The optics used to interpret the signal may be of various forms, including the use of two lenses interposed between an outer diaphragm and a sensor. For example, the lenses may use a revolving symmetrical lens, which the useful part of which is convex, in conjunction with a cylindrical lens which does not create any deflection in a plane parallel to the optical plane. Instead, the optical input is convergent in a plane
25 perpendicular to the parallel plane once received, facilitating translation into numeric, hexadecimal, binary or other digital signaling.

After the smartcard and/or reader perform appropriate public key authentications, the encrypted data is sent back to the DTMF encoder/decoder, enabling the phone, computing device or other unit to validate the authentication transaction. In terms of

security, each transaction uses its own encrypted counter with signals that are different to prevent recording. Within the reader 100, the software is preferably stored in an obscure manner, with each module being preferably software encrypted and decrypted using a unique process, with new keys being transmitted to prevent disassembly or decompilation of the software or portions thereof. Sensors within the unit may be used to detect excessive use of heat or power, representing some form of misconduct which would be reported during the next transaction with all information needed to prevent further usage.

The device 100 preferably includes its own liquid crystal display, facilitating the readout of certain information, such as authorization numbers, payment authorization, serialization, or data regarding check payment or Visa/MasterCard/American Express authorization numbers. Such information would be linked to an amount of purchase or details on an item order and paid once the bank has issued an authorization on the transaction.

Figure 4A is a flow diagram showing the first portion of a preferred device registration process according to the invention. Figure 4B is a flow diagram which illustrates the remaining portion of the preferred device registration process. The procedure commences with the insertion of the smartcard at 402. At block 404, the device interrogates the smartcard, comparing the digital signature in order to validate the authentication procedure. If the signature is correct, block 406, encryption of the digital signature proceeds at block 412. If the signature is not correct, an entry is made into the device memory at 408, and, in the preferred embodiment, the device is frozen in terms of operation until an authorized user unlocks the device at 409, and the process ends at 410.

The encryption of the digital signature at block 412 preferably uses the device's serial identification/session key derived at block 413. At block 414, a query is made to determine if the signature has previously been stored in the device memory. If it has, the registration process has already been completed for this smartcard (block 416), and the device is authenticated at 418. If, however, the signature has not been previously been stored, storage of an encrypted digital signature into the device memory history log occurs at 420.

At block 422, a query is made to determine how many times the personal identification number (PIN) has been entered into the device. If, in this example, it is greater than three, an entry is made into the device memory at 424, and the device is locked out for a predetermined period of time, such as 24 hours, the process ends at 430.

5 If fewer attempted PINs have been entered, a PIN is entered from the keyboard at 432 sent to the smartcard for validation at 434. A test is made at 436 to determine if the PIN is correct. If it is not, the process essentially starts over. If the PIN is correct, however, query is made at 440 to determine if the device is biometrics equipped. If so, the biometric data are acquired at block 450. If not, the user stores personal information that

10 will be linked to smartcard usage at block 442. The device serial number is recovered at 444, either as a public key and/or encrypted biometric data in the form of a public key. At 446, the encrypted personal data and public key are stored in the device memory.

At block 452, having acquired biometric data at 450, the device serial ID and optional atomic time are used as a session key. At block 454 the biometric data are

15 encrypted. This encryption may occur in the device or in a smartcard dedicated to biometric usage, and process passes to block 442. The storage of the encrypted biometric data into the smartcard occurs at block 456. This may occur as permanent storage in some form of non-volatile memory or, alternatively, temporary storage may be transferred into random-access memory (RAM), at 458.

20 Optionally, a third-party phone number may be recovered from the smartcard if, for example, biometric data is unavailable. At 462, the user pushes the SEND button on the device keyboard, causing a third party number to be sent via DTMF modulation or the other schemes disclosed herein. The DTMF data is received from the third party, along with public key session and other information at 466. At block 468, the third party

25 signature is compared to the third party signature or biometric information stored on the card. At 470, a check is made to determine whether the third party signature is authentic. If not, an entry is logged into the memory of the device at 472, and the device is locked until administrative personnel are called upon to unlock it. The process ends at 476.

At block 478, atomic time is recovered for usage in session key generation. At

480, the biometric and/or personal information with third-party public key and/or session key are encrypted at 480 (EB), and the encoded EB information is transmitted via DTMF or other appropriate signaling at 482. In particular, at 484, the EB is transmitted to a third-party, with a log being entered into the device memory. This completes the registration process, with the device being ready to use at 488, and terminating at 490.

Figure 5A is the first party of a flow diagram used to illustrate the preferred way in the device is used according to the invention. Figure 5B is a flow diagram illustrating the remaining functional steps of the usage process. The sequence begins at 502, with a user selecting the smartcard intended for use. At 504, an interrogation is made by the device to determine whether the digital signature is valid to permit authentication. If the signature is correct, at 506, encryption of the digital signature occurs at 512 using the device serial ID as a session key (513). If the signature is not correct, an entry log is made into the memory of the device at 508, and the device is locked until administrative personnel unlock the device, and the process terminates at 510.

At 514, a query is made to determine if the encrypted signature is already stored in the memory of the device. If not, control passes to block 516, awaiting the registration process described with reference to Figures 4A and 4B. If the signature has been stored, and the temp set PIN entry are sufficiently low at 522 a PIN is received from the keyboard at 532. If the number of PIN entries is too high, however, a log is made in the memory of the device at 524, an operation is locked for a determined period of time such as 24 hours at 528 and the process ends at 530.

Once the PIN is input from the keyboard at 532, it is sent to the smartcard for verification at 534. At 536, a check is made to determine whether a PIN is made. If not, the process essentially starts over at block 504. If the PIN is correct, however, control passes to point 538 and onto block 540 where a test is made to determine whether the device is biometrics equipped. If so, the biometrics data are acquired at 550. Optionally, at 552, the device serial ID and atomic time are used as a session key. The biometric data are decrypted at 554, and a test is made at 556 to determine whether the authentication should proceed based upon the decrypted biometric data. If not, the control resumes at

550 with the acquisition of further biometric data, as necessary.

If the biometric data are valid, however, the device is ready to receive data from the light sensor or DTMF decoder at 558. The user initiates the process using the keyboard on the device at 560 to accept sensor data when ready. At 562, the data is
5 received from the sensors, public key and/or session key, including the card information, payment terms, amount of transaction, and so forth.

At 564, personal identification is decrypted and atomic time is recovered at 566 for usage in generating a session key. Personal data are encrypted when received at 570, along with public key, session keys, and third-party public keys. At 572, a code in
10 DTMF of infrared signals is used to encrypt the personal data which is sent to the third-party at 574. The third-party sends back an acknowledgement or refusal of the transaction at 576 and the transaction is recorded on the smartcard 578. A log is made in the memory of the device at 580, and the device is ready for use in a new operation at 582. The session terminates at 584.

15 Figure 6A is a flow diagram which illustrates a preferred process associated with personal data modification utilizing the device according to the invention. The modification process continues in the flowchart of Figure 6B. The process begins at 602 with the user selection of the smartcard. At 604, the device interrogates the smartcard digital signature to validate authentication (604). If the signature is correct (606),
20 encryption of the digital signature occurs at 616, with the device serial ID being used to generate a session key (613). If the signature is not correct, however, an entry is logged in the memory of the device at 608, and the device is locked until administrative personnel are called upon to unlock it at 609, and the process terminates at 610.

Assuming the digital signature has passed through encryption at 616, storage of
25 the smartcard encrypted digital signature in the device and history log occurs at 620. At 622, it is asked whether the personal identification number (PIN) has only been attempted once or a few number of times. If entry is attempted more than a predetermined number of times, such as three or more, a log is made in the device at 624 and it is locked for a predetermined period of time, such as 24 hours at 628. The process terminates at 630. If

only one or a few attempts have been made at PIN entry, the pin is entered from the keyboard at 632, and sent to the smartcard for validation at 634. At 636, a test is made to determine if the PIN is correct. If not, the above process essentially repeats, with control being returned to block 604. Assuming, however, the correct pin has been entered, the question is asked at 640 as to whether the device is biometrics equipped. If so, the biometric data are acquired at 650. If not, the user may store personal identification which will be linked to smartcard usage, including billing address, delivery address, social security, date of birth, limit of payment, credit report, signature, and so forth at 670. The device recovers the serial number for use in generating a public key (and/or encrypted biometric data) at 680. At 690, the personal data are encrypted along with public key information, and the result is stored into the memory of the device.

The encrypted biometric data are also stored in the smartcard and/or inside the device if no biometric data are available at 656. At 658, the device is ready to be used for a new operation, and the process ends at 660.

The invention is not limited in terms of usage, and is therefore applicable to at least the following types of transactions:

- * ID including passports; Identity cards; medical, corporate, and social security,
- * electronic vote based on smartcard technology,
- * TV satellite, cable ordering, payment,
- * any media (TV, computer, DVD, VHS, streaming video, or audio...) advertising payments,
- * internet transactions and authentications,
- * computer authentication and transactions,
- * specific Web application that need authentication (email authentication, or bank authentication transaction),
- * authentication based on data usage or rules (policy) (copyrighted material music, DVD, files, movies, streaming...),
- * public and/or private utilities services such as telephone invoicing, electricity invoicing, water invoicing, gas invoicing, retail outlet gas stations,

* security authentication access (governmental institutions...), hotel industry, entertainment including movies theatres, music/music events, entertainment parks, private and /or gated community, airlines industry (airplane ticket), highway toll, healthcare industry, parking payment. car rental, rental, metro ticket,

- 5 * door opener (home, car), physical security, home security, car security,
 * Payment in physical retail location,
 * ATM cash transaction, (in this case the ATM machine does not need to have any keyboard...),

- * software applications or games usage authentication,
10 * OS usage authentication,
 * lotto, or gaming (casino...) applications based on the payment and the storage of possible personal data,
 * payment on automated machine such as beverage/candy/food machine,
 * Prepaid debit/credit card for micro payment,
15 * The use of a debit/credit card as a phone card,

In addition, the device may further be interconnected to existing accounting software, to memorize the history of card usage and send detailed and itemized balance on all payment collected via software or by phone.

- This device can also return funds to the smartcard holder and notify the bank.
20 This device permit also cache authorization storage based on preapproved amount link to the amount allowing users, to make multiple purchase based on one single authorization number. Providing full payment guaranteed to the merchant. This device will allow multiple credit card issuers, and will handle multiple authorization as well. It further permits complete decentralization of credit report, allowing the device to maintain his/her
25 own credit report.

As an alternative to the use of a separate or independent display (CRT or LCD) and keyboard, the plug-in of Figure 7 may be used. The device is essentially a headset including a smartcard reader, preferably with 2 biometric sensors, one for the voice and the other one for the fingerprint. This is a highly secure device, including a timestamped

Private Key is generally locally and linked to the biometric information. The smartcard used may be a payment card or any service card (i.e., SIM or 7816 size). Up to 5 or more smartcard may be read simultaneously.

In the preferred configuration of this embodiment, the biometric headset include a
5 (cryptographic) processor to perform elliptic curves and random number generator. A dedicated ASIC/DSP sends and receives the DTMF/FSK signals. In addition to other advantages, the system can deliver a vocal instruction to the head set and receive the voice as a second biometric identification from the microphone of the headset. The device is battery operated with a backup. Other features include an atomic time clock and
10 software that can be updated by way of a smartcard (SIM or 7816 size) javacard or DTMF/FSK. The amount of memory is optional. Policy (in encrypted XML) considerations may also be stored on the smartcard.

When the headset is attached, the associated PDA, computer, or phone keyboard sends DTMF signals which are recognized by the device. PDA or phone screen can be
15 updated thru a WAP application link to a vocal server.

This system takes advantage of Identity-based Encryption (IBE) utilizing biometric usage and timestamping technology. At least four algorithms may be used.

1. Setup

A user, "Bob," generates sys-params and master key. To initialize an IBE
20 security, a key generator picks an elliptic curve, a secret S and a point P on the curve using a random number generator. The secret S is the biometric data so nothing can compromise the system.

2. Encrypt

The sender, Alice, during handshaking receive from bob the public parameters, P
25 and $S \cdot P$, (the product of bob's S and P), Bob's identity (this might, for example, be the "phone number" + T where T is the key expiration).

Alice, to encrypt a message to Bob, first hashes Bob's identity to a point on the elliptic curve IDBob. She then picks a random r and calculates a key k where $k = \text{Pair}$

$(R \cdot ID_{Bob}, S \cdot P)$

Alice then sends to Bob $E_k[Message]$, the message encrypted with k . She also sends him the product $R \cdot P$.

3. Key Generation

- 5 When Bob receives the message, retrieve s from bob biometric data, recover and compare T locally (key expiration stored during handshaking) and calculates $S \cdot ID_{Bob}$ and this value is his private key.

4. Decrypt

After receiving the message and a key, Bob can recover the key k by calculating:

10

$$k = \text{Pair}(S \cdot ID_{Bob}, R \cdot P)$$

which, because of the properties of bilinear maps, is the same as the key Alice used to encrypt the message:

15

$$k = \text{Pair}(R \cdot ID_{Bob}, S \cdot P)$$

- Using k , Bob decrypts the message. As Bob is the only person with this private key (biometric), $S \cdot ID_{Bob}$, no one else can calculate k . T = key expiration calculated from the (atomic) timestamped clock
- 20

I claim: